[DISCUSSION DRAFT]

113TH CONGRESS
1ST SESSION

H. R. _____

To amend title 18, United States Code, to provide for additional restrictions on fraud and related activity in connection with computers, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To amend title 18, United States Code, to provide for additional restrictions on fraud and related activity in connection with computers, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "_____ Act of 2013".

TITLE I—CRIMINAL PROVISIONS

SEC. 101. PROTECTING U.S. BUSINESSES FROM FOREIGN ESPIONAGE.

Section 1831(a) of title 18, United States Code, is amended, in the matter after paragraph (5), by striking ''15 years'' and inserting ''20 years''.

SEC. 102. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS AS RICO PREDICATE.

Section 1961(1)(B) of title 18, United States Code, is amended by inserting after ''section 1029 (relating to fraud and related activity in connection with access devices), section 1084 (relating to the transmission of gambling information),'' the following: ''section 1030 (relating to fraud and related activity in connection with computers),''.

SEC. 103. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended as follows:

(1) TRAFFICKING IN PASSWORDS.—In subsection (a), by striking paragraph (6) and inserting the following:

''(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information or means of access through

which a protected computer as defined in subparagraphs (A) and (B) of subsection (e)(2) may be accessed without authorization; or''.

(2) CONSPIRACY AND ATTEMPT.—In subsection (b), by inserting ''for the completed offense'' after ''punished as provided' ''.

(3) PENALTIES.—By striking subsection (c) and inserting the following:

''(c) The punishment for an offense under subsection (a) or (b) of this section is—

''(1)(A) except as otherwise provided in this paragraph, in the case of an offense under subsection (a)(5)(A) of this section, if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both;

''(B) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A) of this section, if the offense caused—

''(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only,

loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

''(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

''(iii) physical injury to any person;

''(iv) a threat to public health or safety;

''(v) damage affecting a computer used by, or on behalf of, an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

''(vi) damage affecting 10 or more protected computers during any 1-year period;

''(C) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(B), if the offense caused a harm provided in clause (i) through (vi) of subparagraph (A) of this subsection; or

"(D) a fine under this title, imprisonment for not more than 1 year, or both, for any other offense under subsection (a)(5) of this section;

"(2) a fine under this title or imprisonment for not more than 20 years, or both, in the case of an offense under—

"(A) subsection (a)(1) of this section; or

"(B) subsection (a)(4) of this section;

"(3) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under—

"(A) subsection (a)(6) of this section;

"(B) subsection (a)(7) of this section;

"(4)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than 3 years, or both, in the case of an offense under subsection (a)(2); or

"(B) a fine under this title or imprisonment for not more than 10 years, or both, in the case of an offense under paragraph (a)(2) of this section, if—

"(i) the offense was committed for purposes of commercial advantage or private financial gain;

"(ii) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

"(iii) the value of the information obtained, or that would have been obtained if the offense was completed, exceeds $5,000; or

"(5) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(3) of this section;".

(4) EXCEEDS AUTHORIZED ACCESS.—In subsection (a), by striking paragraph (2) and inserting the following:

"(2) intentionally—

"(A) accesses a computer without authorization, and thereby obtains—

"(i) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

"(ii) information from any department or agency of the United States; or

"(iii) information from any protected computer; or

"(B) exceeds authorized access, and—

"(i) thereby obtains from a computer information defined in paragraph (A)(i) through (iii); and

"(ii) the offense—

"(I) involves information that exceeds $5,000 in value;

"(II) was committed for purposes of obtaining sensitive or non-public information of an entity or another individual (including such information in the possession of a third party), including medical records, wills, diaries, private correspondence, financial records, photographs of a sensitive or private nature, trade secrets, or sensitive or non-public commercial business information;

"(III) was committed in furtherance of any criminal act in violation of the Constitution or laws of the

United States or of any State, unless such state violation would be based solely on the obtaining of information without authorization or in excess of authorization; or

''(IV) involves information obtained from a computer used by or for a government entity; or''.

(5) FORFEITURES.—By striking subsections (i) and (j) and inserting the following:

''(i) CRIMINAL FORFEITURE.—(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

''(A) such person's interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of such violation; and

''(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation.

''(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

''(j) CIVIL FORFEITURE.—(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them:

''(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section.

''(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section.

''(2) Seizures and forfeitures under this subsection shall be governed by the provisions in chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section

981(d) of title 18, United States Code, shall be performed by such officers, agents and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.''.

(6) DEFINITION.—In subsection (e)(6), by inserting after ''alter'' the following: '', even if the accesser may be entitled to obtain or alter the same information in the computer for other purposes''.

SEC. 104. DAMAGE TO CRITICAL INFRASTRUCTURE COMPUTERS.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''SEC. 1030A. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

''(a) DEFINITIONS.—In this section—

''(1) the terms 'computer' and 'damage' have the meanings given such terms in section 1030; and

''(2) the term 'critical infrastructure computer' means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including—

"(A) gas and oil production, storage, and delivery systems;

"(B) water supply systems;

"(C) telecommunication networks;

"(D) electrical power delivery systems;

"(E) finance and banking systems;

"(F) emergency services;

"(G) transportation systems and services; and

"(H) government operations that provide essential services to the public.

"(b) OFFENSE.—Whoever, during and in relation to a felony violation of section 1030, intentionally causes or attempts to cause damage to a critical infrastructure computer, and such damage results in (or, in the case of an attempt, would, if completed have resulted in) the substantial impairment—

"(1) of the operation of the critical infrastructure computer, or

"(2) of the critical infrastructure associated with the computer,

shall be fined under this title, imprisoned for not more than 30 years, or both.

"(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place on probation any person convicted of a violation of this section;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation section 1030;

''(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy

statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''Sec. 1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. 105. PREPAREDNESS OF FEDERAL COURTS TO PROMOTE CYBER SECURITY.

Not later than 180 days after the date of enactment of this Act, the Administrative Office of the United States Courts shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report providing an assessment of the vulnerability of the Federal courts' computer and network systems to cyber intrusion and attacks that includes recommendations on changes and improvements to the Federal courts' computer and network security systems to address any deficiencies in computer and network security.

SEC. 106. AUTHORIZATION OF NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE.

The Attorney General is authorized to establish the National Cyber Investigative Joint Task Force, which shall be charged with coordinating, integrating, and shar-

ing information related to all domestic cyber threat investigations.

TITLE II—DATA SECURITY AND BREACH NOTIFICATION

SEC. 201. NOTIFICATION OF INFORMATION SECURITY BREACH.

(a) IN GENERAL.—Except as otherwise provided in this section, a covered entity shall notify its customers of a security breach affecting such customers not later than [14] days after that security breach.

(b) ADDITIONAL NOTIFICATION REQUIREMENTS.—

(1) THIRD-PARTY ENTITIES.—In the event of a security breach of a system maintained by a third-party entity, such third-party entity shall notify such covered entity of the security breach.

(2) SERVICE PROVIDERS.—If a service provider becomes aware of a security breach involving data in electronic form containing personal information that is owned or possessed by a covered entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, such service provider shall notify the covered entity who initiated such connection,

transmission, routing, or storage if such covered entity can be reasonably identified.

(3) COVERED ENTITY NOTIFICATION.—Upon receiving notification from a third-party entity or a service provider under this subsection, a covered entity shall provide notification as required under subsection (a) or subsection (d).

(c) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT OR NATIONAL SECURITY PURPOSES.—

(1) LAW ENFORCEMENT.—If a Federal [or State] law enforcement agency determines that the notification required under subsection (a) would impede a civil or criminal investigation, such notification shall be delayed upon the request of the law enforcement agency for any period which the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent request, revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent request if further delay is necessary.

(2) NATIONAL SECURITY.—If a Federal national security agency or homeland security agency determines that the notification required under this section would threaten national or homeland secu-

rity, such notification may be delayed upon the written request of the national security agency or homeland security agency for any period which the national security agency or homeland security agency determines is reasonably necessary. A Federal national security agency or homeland security agency may revoke such delay or extend the period set forth in the original request made under this subparagraph by a subsequent written request if further delay is necessary.

(d) MAJOR SECURITY BREACH; NOTICE TO LAW ENFORCEMENT.—A covered entity shall notify the United States Secret Service or the Federal Bureau of Investigation of the fact that a major security breach has occurred not later than ⟦72 hours⟧ after such major security breach has occurred.

(e) CONTENT OF NOTIFICATION.—Regardless of the method by which notification is provided to an individual under subsection (a) with respect to a security breach, such notification, to the extent practicable, shall include—

(1) the date, estimated date, or estimated date range of the security breach;

(2) a description of the personal information that was accessed and acquired, or reasonably believed to have been accessed and acquired, by an un-

authorized person as a part of the security breach; and

(3) information that the individual can use to contact the covered entity to inquire about—

(A) the security breach; or

(B) the information the covered entity maintained about that individual.

(f) TREATMENT OF PERSONS GOVERNED BY OTHER FEDERAL LAW.—A covered entity who is in compliance with any other Federal law that requires such covered entity to provide notification to individuals following a security breach shall be deemed to be in compliance with this section.

SEC. 202. CIVIL REMEDIES.

(a) CIVIL ACTION.—The Attorney General may in a civil action obtain a civil penalty of not more than $500,000 from any covered entity that engages in conduct constituting a violation.

(b) SPECIAL RULE FOR INTENTIONAL VIOLATIONS.—If the violation of this title described in subsection (a) is intentional, the maximum civil penalty is $1,000,000.

(c) NO PRIVATE CAUSE OF ACTION.—Nothing in this title shall be construed to establish a private cause of action against a person for a violation of this title.

SEC. 203. DEFINITIONS.

In this title:

(1) SECURITY BREACH.—The term ''security breach'' means unauthorized access and acquisition of data in electronic form containing personal information.

(2) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means a commercial entity that acquires, maintains, stores, or utilizes personal information.

(B) EXEMPTIONS.—The term ''covered entity'' does not include the following:

(i) Financial institutions subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(ii) An entity covered by the regulations issued under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191) to the extent that such entity is subject to the requirements of such regulations with respect to protected health information.

(3) DATA IN ELECTRONIC FORM.—The term ''data in electronic form'' means any data stored electronically or digitally on any computer system or

other database and includes recordable tapes and other mass storage devices.

(4) MAJOR SECURITY BREACH.—The term ''major security breach'' means any security breach involving—

(A) means of identification pertaining to 10,000 or more individuals is, or is reasonably believed to have been acquired;

(B) databases owned by the Federal Government; or

(C) means of identification of Federal Government employees or contractors involved in national security matters or law enforcement.

(5) MEANS OF IDENTIFICATION.—The term ''means of identification'' has the meaning given that term in section 1028 of title 18, United States Code.

(6) PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''personal information'' means an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(i) Social Security number.

(ii) Driver's license number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

(iii) Financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

(B) EXEMPTIONS FROM PERSONAL INFORMATION.—

(i) PUBLIC RECORD INFORMATION.—Personal information does not include information obtained about an individual which has been lawfully made publicly available by a Federal, State, or local government entity or widely distributed by media.

(ii) ENCRYPTED, REDACTED, OR SECURED DATA.—Personal information does not include information that is encrypted, redacted, or secured by any other method or technology that renders the data elements unusable.

(7) SERVICE PROVIDER.—The term ''service provider'' means an entity that provides electronic data transmission, routing, intermediate, and transient storage, or connections to its system or network, where such entity providing such services does not select or modify the content of the electronic data, is not the sender or the intended recipient of the data, and does not differentiate personal information from other information that such entity transmits, routes, stores, or for which such entity provides connections. Any such entity shall be treated as a service provider under this title only to the extent that it is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections.

(8) THIRD-PARTY ENTITY.—The term ''third-party entity'' means an entity that has been contracted to maintain, store, or process data in electronic form containing personal information on behalf of a covered entity who owns or possesses such data.

SEC. 204. EFFECT ON FEDERAL AND STATE LAW.

The provisions of this title shall supersede any provision of the law of any State, or a political subdivision

thereof, relating to notification by a covered entity of a security breach.